REMARKS

This amendment is in response to the Non-Final Office Action dated October 27, 2008 ("the Office Action"). Claims 1-11, 13-16, 18-22, and 24-26 are pending in the application. Claims 12, 17, and 23 have been cancelled without prejudice or disclaimer. Claims 1, 2, 5, 6, 10, 12-14, 16, 18, and 21-26 have been amended. No new matter has been added. Support for the claim amendments can be found at least at paragraph 016 of the original specification.

The Objections To The Specification Should Be Withdrawn

The Office has objected to the specification as failing to provide sufficient antecedent support for the claimed subject matter.

In particular, the Office takes the position that claims 25 and 26 are directed to a computer-readable medium but that the term "computer-readable medium" in not defined in the specification. Applicants respectfully note in response that the term "computer-readable medium" is well-known in the art. Further, the term is used in the specification. For example, the original specification at paragraph 0020 states, "In such a system, the remote computing platform may include a computer-readable medium containing computer-readable instructions capable of instructing the platform to receive a request for access to an information network." (Emphasis Added). It is respectfully submitted that the term "computer-readable medium" would be well understood by a person of ordinary skill in the art. In addition, claims 25 and 26 have been amended to include a computer-readable storage medium. A computer-readable storage medium is statutory subject matter. As such, the Applicants respectfully request withdrawal of this reason for objection.

The Office further takes the position that the term "unique" is used in the claims but there is no clear and explicit definition of the word in the specification. Applicants note in response that the word "unique" has been removed in the current claim amendments without prejudice or disclaimer. As such, the Applicants respectfully request withdrawal of this reason for objection.

Claims 1 and 2 are Allowable

The Office has rejected claims 1 and 2 under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. 6,731,731 ("Ueshima") in view of U.S. Patent No. 7,050,423 ("Schneider"). Applicants respectfully traverse the rejections.

The cited portions of Ueshima and Schneider, individually or in combination, do not disclose or suggest the specific combination of claim 1. For example, the cited portions of the above-cited references fail to disclose or suggest generating a first network generated credential comprising network specific information associated with a connection of a user, replacing a first credential received from the user with the first network generated credential, and considering the first network generated credential in connection with making an authentication decision for the user, as in claim 1.

In contrast to claim 1, the cited portions of Ueshima describe a method of authenticating a user that includes matching a phone number of the user's device with a table of phone numbers of registered users. *See* Ueshima, column 10, lines 7-10. If the user's phone number matches a registered user's phone number, a password generating unit sends a password to the user. *See* Ueshima, column 10, lines 20-29. If the user transmits a password to the authentication system that matches the password that was sent to the user, the authentication system authenticates the user. *See* Ueshima, Abstract. That is, the transmitted user password replaces the user's phone number as the basis for authentication. The cited portions of Ueshima define a password as a "combination of numerals, alphabets, symbols, katakana, and other characters." *See* Ueshima, column 10, lines 30-34. The cited portions of Ueshima do not disclose network specific information. Applicants respectfully submit that replacing the user's phone number with a password is different from replacing a credential with a network generated credential comprising network specific information. Therefore, the cited portions of Ueshima do not disclose or suggest generating a first network generated credential comprising network specific information associated with a connection of a user, replacing a first credential received from the user with the first network generated credential, and considering the first network generated credential in connection with making an authentication decision for the user, as in claim 1.

In further contrast to claim 1, the cited portions of Schneider describe a method for accepting or rejecting service requests based on the service capabilities and service permissions of the system and the customer as delivered through a certificate. *See* Schneider, Abstract, claim

1, and column 2, lines 59-67. That is, Schneider's certificate is the only basis for the acceptance or rejection of a service request. The cited portions of Schneider do not mention the topic of replacing credentials with network specific information. Therefore, the cited portions of Schneider does not disclose or suggest generating a first network generated credential comprising network specific information associated with a connection of a user, replacing a first credential received from the user with the first network generated credential, and considering the first network generated credential in connection with making an authentication decision for the user, as in claim 1. Hence, claim 1 is allowable. Claim 2 depends from claim 1. Accordingly, claim 2 is allowable, at least by virtue of its dependence from claim 1. Further, claim 2 recites additional elements not disclosed or suggested by the cited portions of the above-cited references.

For example, the cited portions of Ueshima and Schneider fail to disclose or suggest generating a second network generated credential comprising network specific information associated with a connection of a different user, replacing a second credential received from the different user with the second network generated credential, where the second network generated credential does not match the first network generated credential, and considering the second network generated credential in connection with making an authentication decision for the different user, as in claim 2. The cited portions of Ueshima disclose a method of separately authenticating individual users even if the same terminal is used by a plurality of users by using the user's name upon authentication. *See* Ueshima, column 3, lines 21-22 and column 17, lines 10-12. That is, the cited portions of Ueshima disclose distinguishing between individual users by a separate authentication based on user name, not network specific information. In addition, the cited portions of Schneider do not disclose or suggest replacing credentials with network specific information to authenticate users. Therefore, the cited portions of Ueshima and Schneider do not disclose or suggest generating a second network generated credential comprising network specific information associated with a connection of a different user, replacing a second credential received from the different user with the second network generated credential, where the second network generated credential does not match the first network generated credential, and considering the second network generated credential in connection with making an authentication decision for the different user, as in claim 2. For at least this additional reason, claim 2 is allowable.

Claims 3-11, 13-16, 18-22, and 24-26 are Allowable

The Office has rejected claims 3-26 under 35 U.S.C. § 103(a), as being unpatentable over Ueshima in view of Schneider in further view of Official Notice. Claims 12, 17, and 23 have been cancelled without prejudice or disclaimer. Applicants respectfully traverse the remainder of the rejections.

Claims 3-11 and 13 depend from claim 1. As explained above, the cited portions of Ueshima and Schneider fail to disclose or suggest at least one element of claim 1. Therefore, claims 3-11 and 13 are allowable, at least by virtue of their dependence from claim 1.

Claim 4 is distinct from any teaching or suggestion of the cited combination. Applicants respectfully disagree that there exists a motivation to use a cable connection in place of the telephone connection of Ueshima or that such a system would even function. Simple substitution of a cable connection in place of the telephone connection of Ueshima would lead to a non-working system. For example, part of Ueshima cited by the Office describe that the user placed a call to the CTI system. *See* Office Action, paragraphs 8.1 and 8.2. If a cable connection was substituted for the telephone connection, it would not be possible to place a call. Claim 4 recites the connection of the user comprises a link at least partially supported by a cable modem. Claim 4 is allowable for at least this additional reason.

With respect to Claim 5, the Office takes the position that Ueshima at col. 3, lines 38-41, indicates that CTI device or other device generates the password. However, claim 5 recites "utilizing a network node to generate the network specific information." The password discussed in Ueshima cannot be equated with the network specific information of claim 5 at least because the password of Ueshima is not generated after generating a common user credential from the user. Claim 5 is allowable for at least this additional reason.

With respect to Claim 10, the Office takes the position that Ueshima at col. 3, lines 38-41 indicates that CTI device or other device generates the password. However, claim 10 recites "utilizing a network node to generate the network specific information". The password discussed in Ueshima cannot be equated with the unique credential of claim 10 at least because the password of Ueshima is not generated after receiving a common user credential from the user. Claim 10 is allowable for at least this additional reason.

The cited portions of Ueshima and Schneider, individually or in combination, do not disclose or suggest the specific combination of claim 14. For example, the cited portions of the above-cited references fail to disclose or suggest generating a network generated credential comprising network specific information associated with a connection of a user, replacing a credential received from the user with the network generated credential, and considering the network generated credential in connection with making an authentication decision for the user, as in claim 14.

In contrast to claim 14, the cited portions of Ueshima describe a method of authenticating a user that includes matching the phone number of the user's device with a table of phone numbers of registered users. *See* Ueshima, column 10, lines 7-10. If the user's phone number matches a registered user's phone number, a password generating unit sends a password to the user. *See* Ueshima, column 10, lines 20-29. If the user transmits a password to the authentication system that matches the password that was sent to the user, the authentication system authenticates the user. *See* Ueshima, Abstract. That is, the transmitted user password replaces the user's phone number as the basis for authentication. The cited portions of Ueshima define a password as a "combination of numerals, alphabets, symbols, katakana, and other characters." *See* Ueshima, column 10, lines 30-34. The cited portions of Ueshima do not disclose network specific information. Applicants respectfully submit that replacing the user's phone number with a password is different from replacing a credential with a network generated credential comprising network specific information. Therefore, the cited portions of Ueshima do not disclose or suggest generating a network generated credential comprising network specific information associated with a connection of a user, replacing a credential received from the user with the network generated credential, and considering the network generated credential in connection with making an authentication decision for the user, as in claim 14.

In further contrast to claim 14, the cited portions of Schneider describe a method for accepting or rejecting service requests based on the service capabilities and service permissions of the system and the customer as delivered through a certificate. *See* Schneider, Abstract, claim 1, and column 2, lines 59-67. That is, Schneider's certificate is the only basis for the acceptance or rejection of a service request. The cited portions of Schneider do not mention the topic of replacing credentials with network specific information. Therefore, the cited portions of Schneider do not disclose or suggest generating a network generated credential comprising

network specific information associated with a connection of a user, replacing a credential received from the user with the network generated credential, and considering the network generated credential in connection with making an authentication decision for the user, as in claim 14. Hence, claim 14 is allowable. Claims 15-16, 18-22, and 24 depend from claim 14. Accordingly, claims 15-16, 18-22, and 24 are allowable, at least by virtue of their dependence from claim 14. Further, the dependent claims recite additional elements not disclosed or suggested by the cited portions of the above-cited references.

The cited portions of Ueshima and Schneider, individually or in combination, do not disclose or suggest the specific combination of claim 25. For example, the cited portions of the above-cited references fail to disclose or suggest replacing a credential with a network generated credential comprising network specific information associated with a connection of a user seeking access to an information network and comparing the network generated credential against a stored collection of acceptable credentials, as in claim 25.

In contrast to claim 25, the cited portions of Ueshima describe a method of authenticating a user that includes matching the phone number of the user's device with a table of phone numbers of registered users. *See* Ueshima, column 10, lines 7-10. If the user's phone number matches a registered user's phone number, a password generating unit sends a password to the user. *See* Ueshima, column 10, lines 20-29. If the user transmits a password to the authentication system that matches the password that was sent to the user, the authentication system authenticates the user. *See* Ueshima, Abstract. That is, the transmitted user password replaces the user's phone number as the basis for authentication. The cited portions of Ueshima define a password as a "combination of numerals, alphabets, symbols, katakana, and other characters." *See* Ueshima, column 10, lines 30-34. The cited portions of Ueshima do not disclose network specific information. Applicants respectfully submit that replacing the user's phone number with a password is different from replacing a credential with a network generated credential comprising network specific information. Therefore, the cited portions of Ueshima do not disclose replacing a credential with a network generated credential comprising network specific information associated with a connection of a user seeking access to the information network and comparing the network generated credential against a stored collection of acceptable credentials, as in claim 25.

In further contrast to claim 25, the cited portions of Schneider describe a method for accepting or rejecting service requests based on the service capabilities and service permissions of the system and the customer as delivered through a certificate. *See* Schneider, Abstract, claim 1, and column 2, lines 59-67. That is, Schneider's certificate is the only basis for the acceptance or rejection of a service request. The cited portions of Schneider do not mention the topic of replacing credentials with network specific information. Therefore, the cited portions of Schneider does not disclose replacing a credential with a network generated credential comprising network specific information associated with a connection of a user seeking access to the information network and comparing the network generated credential against a stored collection of acceptable credentials, as in claim 25. Hence, claim 25 is allowable. Claim 26 depends from claim 25. Accordingly, claim 26 is allowable, at least by virtue of its dependence from claim 25.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the references applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the cited art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

1-22-2009
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
TOLER LAW GROUP, INTELLECTUAL PROPERTIES
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)